

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,
Plaintiff,
v.
MUHAMMAD FAHD,
Defendant.

No. CR17-0290RSL

GOVERNMENT'S SENTENCING
MEMORANDUM

The United States of America, by and through undersigned counsel, files this Memorandum in anticipation of the sentencing hearing in this matter. Sentencing is scheduled for September 16, 2021 at 10 am.

I. INTRODUCTION

Defendant Muhammad FAHD is a modern-day cybercriminal who combined his technological expertise with old-school techniques such as bribery, intimidation, and exploitation. For over seven years, FAHD worked tirelessly to breach the network security of AT&T. He did so to run a cybercriminal enterprise that illegally unlocked at least 1.9 million cellular phones from AT&T's network and caused over \$200 million in losses. FAHD's scheme not only caused massive losses to AT&T and its shareholders, but also irreparably damaged the lives of the young and impressionable AT&T employees whom he recruited and exploited.

1 For the reasons set forth below, the United States recommends that the Court
2 sentence FAHD to fifteen years' imprisonment, enter a restitution judgment in the
3 amount of \$200,620,698, and order FAHD to forfeit a sum of money in the amount of
4 \$5,338,430.

5 II. BACKGROUND

6 A. The Unlocking Scheme

7 AT&T Mobility LLC ("AT&T") is a company headquartered in Atlanta, Georgia.
8 AT&T sells cellular telephones, including iPhones, and it offers monthly voice and data
9 plans for use with the phones on AT&T's wireless network. Plea Agreement ("PA"), 5.
10 Cellular phones such as iPhones cost hundreds of dollars. To make the phones more
11 affordable, during the relevant period, AT&T subsidized the purchase cost of phones or
12 sold phones to customers under installment plans. *Id.* In either case, customers were
13 required to enter contracts that bound them to AT&T's wireless network for a set period.
14 *Id.* In cases in which AT&T subsidized the purchase of phones, a portion of the
15 payments under the service contracts covered the part of the cost of phones that AT&T
16 had subsidized. Presentence Report ("PSR"), ¶10.

17 "Unlocking" a cellular telephone refers to removing software that limits the phone
18 to being used on a carrier's cellular telephone network – in this case, AT&T's network.
19 PA, 6. AT&T, like other major carriers, installed locking software because AT&T
20 typically sold cellular phones either at highly subsidized prices, or on installment plans.
21 *Id.* AT&T counted on recovering the cost of cellular phones, as part of the payments that
22 customers made under service contracts or installment plans to purchase the phones. *Id.*
23 Both service contracts and installment plans typically had two-year terms.

24 As cellular telephones have proliferated over the last two decades, a substantial
25 underground market has developed based on the illegal unlocking of cellular telephones.¹
26 In many cases, this is accomplished by bribing employees of telecommunication carriers

27
28 ¹ See, e.g., The Secret World of Stolen Smartphones, Where Business Is Booming,
<https://www.wired.com/2014/12/where-stolen-smart-phones-go/> (last checked 12/4/2020).

1 to unlock cellular telephones that are not eligible for unlocking, or by hacking into a
2 carrier's computer systems and using the resulting access to unlock cellular telephones
3 that are not eligible for unlocking. When cellular telephones are improperly unlocked,
4 carriers like AT&T often incur significant losses. PA, 6; PSR, ¶11.

5 First, customers who have unlocked their cellular telephones often walk away
6 from the service plans or installment plans that covered the cost of their phones (and
7 instead enter into new typically cheaper service contracts with different companies). *See*
8 PSR, ¶11. In such cases, the original carrier loses the remaining portion of the cost of the
9 cellular telephone. PA, 6; PSR, ¶11. This may be as much as the entire cost of a phone,
10 where a customer obtained the phone with the intent of immediately unlocking it.

11 Second, there is a large market in stolen cellular telephones. To have value in this
12 market, stolen cellular phones must be disconnected from their initial purchasers' service
13 plans. As result, one step that sellers and resellers of stolen phones (who often operate at
14 considerable scale) take is unlocking the phones. Once unlocked, the cellular telephones
15 are resold to customers, often overseas.² As with customers unlocking their own
16 telephones, unlocking of stolen cellular telephones by participants in this illicit market
17 results in cellular phone companies, such as AT&T, losing the remaining portion of the
18 cost of the cellular telephones. *See* PSR, ¶11.

19 From approximately April 2012 through approximately September 2017, AT&T
20 used computer programs through which AT&T customer service representatives could
21 submit unlock requests for eligible customers. PA, 6. Only authorized employees
22 connected to AT&T's internal and protected computer network could access the
23 unlocking programs. When a customer service representative submitted an unlocking
24 request through a program, the customer service representative represented to AT&T that
25 the representative (a) was authorized to use the program, (b) was accessing the program
26
27

28 ² *See, e.g.,* Inside The Massive Global Black Market For Smartphones, https://www.huffpost.com/entry/smartphone-black-market_n_3510341 (last checked 12/4/2020).

1 from AT&T's protected network, and (c) had applied AT&T's eligibility criteria to
2 determine that the unlocking request was appropriate. *Id.*, 6-7.

3 From approximately April 2012 until approximately September 2017, FAHD, and
4 others conspired to defraud AT&T by bribing AT&T employees at an AT&T call center
5 in Bothell, Washington ("the Bothell call center"), to unlock over 1.9 million cellular
6 phones for ineligible customers. PA, 6, 8-10. Among other methods, the bribed AT&T
7 employees intentionally introduced malware provided to them by FAHD onto AT&T's
8 computer network via the employees' computer workstations. *Id.*, 8. The malware
9 allowed FAHD to unlock massive numbers of cellular phones, without the authorization
10 of AT&T. *Id.*, 9-10. FAHD also used AT&T employee DeV Vaughn Woods to install
11 unauthorized hardware devices on AT&T's protected network to steal the credentials of
12 customer service representatives and to submit large quantities of unlock requests
13 through AT&T's unlocking programs. *Id.*, 9. Like the malware, the hardware devices
14 allowed members of the scheme, remotely and without authorization, to send data and
15 commands to AT&T's unlocking programs, and thereby altered and impacted the normal
16 functioning of AT&T's unlocking system. *Id.*

17 The bribed AT&T employees did not have authority to unlock the phones in this
18 fashion. By submitting requests to unlock cellular phones that should not have been
19 unlocked, the bribed employees misrepresented to AT&T the eligibility of the phones for
20 unlocking. PA, 7. The bribed AT&T employees knew that customers who owned these
21 unlocked phones could use them on other wireless networks, and that many customers
22 who did so would stop making monthly service plan and/or installment plan payments to
23 AT&T. *Id.*, 7. The bribed AT&T employees thereby defrauded AT&T of the stream of
24 payments that AT&T would have received had the customers completed making
25 payments due under their service and installment contracts. AT&T does not use a bank
26 to finance installment contracts – as a result, the lost payments resulted in massive losses
27 to AT&T itself.

1 **B. Fahd Recruits AT&T Insiders to Carry Out the Scheme**

2 The scheme began in the spring of 2012, when FAHD started recruiting
3 employees at the Bothell call center to perform illegal unlocks. PA, 7; PSR, ¶¶12-13. He
4 used a variety of names when communicating with these representatives, including
5 Frank, Frank Zhang, Frankie, and Muhammad Asif. PA, 7; PSR, ¶13. The Bothell call
6 center employees whom FAHD successfully recruited included Mark Sapatin, Kyra
7 Evans, DeVaughn Woods, and others.

8 FAHD approached Sapatin through Facebook, and offered Sapatin a great deal of
9 money for helping with unlocks. PA, 7; PSR, ¶13. FAHD directed Sapatin to set up new
10 email accounts and to buy a pre-paid cell phone so they could communicate privately.
11 PSR, ¶ 14. FAHD had regular video chats with Sapatin and bragged to Sapatin about
12 how much money he was making. While FAHD was travelling, he gave Sapatin video
13 tours of the luxurious hotels at which he was staying, and showed Sapatin stacks of cash
14 and new watches he purchased. On one occasion, FAHD showed Sapatin one of the
15 handguns in his possession. Here is one of the photos that FAHD sent to Sapatin on
16 approximately August 22, 2012:



26 FAHD directed Sapatin to recruit other employees at the Bothell call center. PA, 7, 9.
27 Sapatin recruited Evans, and the two, in turn, recruited Woods. PSR, ¶19. In addition,
28

1 Sapatin recruited N.L. to join the scheme shortly before the scheme was discovered by
2 AT&T. PA, 9.

3 **C. Phase One of the Scheme**

4 **1. Manually entering IMEIs**

5 FAHD's scheme had two distinct phases. The first phase occurred between July
6 and October 2013. At the outset of the scheme, the conspiracy had to unlock the phones
7 manually by entering groups of international mobile equipment identity ("IMEI")
8 numbers of the phones into AT&T's unlocking system. PA, 8. FAHD would send the
9 AT&T insiders lists of the IMEIs to unlock. PSR, ¶15. Before their shifts ended, the
10 AT&T insiders would email FAHD reports indicating which of the IMEIs had been
11 unlocked successfully. *Id.*

12 FAHD was using the AT&T insiders to provide wholesale unlocking services to
13 retailers who, in turn, sold the illegal unlocks to individual customers. In particular,
14 FAHD provided unlocking services to two online retailers run by P.V. and S.V. The cost
15 to illegally unlock a phone varied during the scheme. Unlocking newer phones that were
16 unlocked within a few hours could cost as much as \$74.99 or more. In contrast,
17 unlocking older phones within more than 24 hours could cost as little as \$1.99. The
18 following is a screenshot from a retail website advertising the sale of the unlocking
19 service, indicating that FAHD could unlock all types of phones, including phones that
20 had been flagged by AT&T as being stolen phones:



Unlock AT&T; iPhone 7 / 7 PLUS [PREMIUM]

\$74.99

Service is a back up method which just started. Please understand it can go offline any time

Supports ATT iPhone models: 2G, 3, 3GS, 4, 4S, 5, 5C, 5S, 6+, 6, 6S, 6S+ SE, 7, 7+

This is a premium service that has 100% **SUCCESS RATE**. Many times orders are rejected by Apple if the phone is in contract, next contract, active on line, etc

If Device blacklisted [lost/stolen/fraud] it is supported on this service. (will work outside of USA only once unlocked)

Timeframe: 1-3 Business Days

Once order is in process. No cancellations can be made.

The AT&T insiders provided FAHD with access not only to sensitive portions of the AT&T's computer systems, but also personally identifiable information about AT&T's customers. This information included phone numbers, geographic information, billing information, and portions of social security numbers. For example, on October 24, 2012, Evans emailed FAHD a list of phone numbers, zip codes and partial social security numbers for 44 customers:

Re: zip and ssn list

From: Yang Knowles <yanghov687@gmail.com>
To: Muhammad Asif <unlockoutlet@gmail.com>
Sent: October 24, 2012 6:01:28 PM PDT
Received: October 24, 2012 6:01:28 PM PDT
Attachments: ###.txt

22834 [REDACTED] 739525-4093 SSN [REDACTED]
41581 [REDACTED] 94014-1552 SSN [REDACTED]
20180 [REDACTED] 07640-1302 SSN [REDACTED]
93130 [REDACTED] 37042-8649 SSN [REDACTED]
32143 [REDACTED] 32817-2661 SSN [REDACTED]
80542 [REDACTED] 93065-4431 SSN [REDACTED]
91765 [REDACTED] 10028-6151 SSN [REDACTED]
80667 [REDACTED] 79106-5128 SSN [REDACTED]
80677 [REDACTED] 79423-0851 SSN [REDACTED]
91774 [REDACTED] 11214-2674 SSN [REDACTED]
85727 [REDACTED] 02125-1037 SSN [REDACTED]
84783 [REDACTED] 60131-2517 SSN [REDACTED]
94929 [REDACTED] 92672-3409 SSN [REDACTED]
84528 [REDACTED] 07002-3016 SSN [REDACTED]
30122 [REDACTED] 20814-6236 SSN [REDACTED]
31857 [REDACTED] 71108-5861 SSN [REDACTED]
81866 [REDACTED] 91324-4206 SSN [REDACTED]
30545 [REDACTED] 33189-3306 SSN [REDACTED]
78623 [REDACTED] 33030-5927 SSN [REDACTED]
51091 [REDACTED] 94502-7949 SSN [REDACTED]
21490 [REDACTED] 75056-5636 SSN [REDACTED]

2. Using Malware to Unlock Phones

In the spring of 2013, AT&T implemented a new unlocking system that made it more difficult for the conspiracy to unlock IMEIs. PA, 8. As a result, FAHD hired software developers to custom-design malware that would give him remote access to AT&T's system so he could unlock phones remotely. PA, 8; PSR, ¶16. To assist with the development process, FAHD directed the AT&T insiders to install surveillance

software that captured information about AT&T's computer system and unlocking procedures. PA, 8; PSR, ¶16.

After a lengthy period of surveillance, FAHD and a software developer were able to design malware for the insiders to test. *See* PSR, ¶17. FAHD provided the insiders with instructions on how to test the various versions of the malware. PA, 8; PSR, ¶17. The following email depicts FAHD giving Sapatin instructions on how to conduct the eighth test of the malware:

TEST8

From: Muhammad Fahd <unlockoutlet@ymail.com>
To: tropoja786@yahoo.com <tropoja786@yahoo.com>
Sent: April 19, 2013 7:40:39 AM PDT
Received: April 19, 2013 7:40:39 AM PDT
Attachments: browser.zip

Download the File , Extract all in a folder , then run the Wbrowser.exe , then goto Snooper on this new browser , login to snooper , once ur logged in on the snooper page , press the start button on browser (dont press it before logging into snooper) , then after pressing the start button , process a iphone unlock with any imei , when that is done , zip the saved folder and send it on yahoo to me !!!

The malware gave FAHD the ability to unlock large numbers of IMEI numbers through the AT&T insiders. Pursuant to FAHD's instructions, the AT&T insiders would activate the malware at the start of every shift. PA, 8. While the AT&T insiders were performing their usual duties, FAHD would use the malware to unlock large volumes of phones. PSR, ¶17.

3. Discovery by AT&T and FAHD's Obstruction of Justice

In October 2013, AT&T discovered the malware and learned that Sapatin, Evans, and N.L. were conducting large quantities of unauthorized unlocks. PA, 9. AT&T investigators interviewed Sapatin and Evans. While Sapatin was being interviewed by AT&T's Asset Protection department, FAHD instructed Evans to destroy evidence of the scheme on her computer:

| | |
|----------------------|---------------------------------------|
| Kyra Evans | Yea what's up |
| Muhammad Fahd | did marc text you on something |
| Kyra Evans | no he didn't |

| | |
|----------------------|---|
| Muhammad Fahd | what is asset protection at att? |
| Kyra Evans | Idk |
| Kyra Evans | I can look tmrw morning |
| Muhammad Fahd | he messaged me saying they are interviewing him |
| Muhammad Fahd | idk what's going on |
| Kyra Evans | Oh at this time of day? |
| Muhammad Fahd | idk what's going with him , hes not telling me straight up , all he said is they investigating |
| Kyra Evans | Can u call me in five minutes |
| Kyra Evans | Are you going to call me? |
| Muhammad Fahd | Clean all files out tomorrow |
| Muhammad Fahd | >From your computer |
| Muhammad Fahd | stay cool |
| Kyra Evans | I'm trying |
| Muhammad Fahd | relax calm ur nerves |
| Kyra Evans | Omg my heart is beating so fast |
| Muhammad Fahd | don't go paranoid |
| Muhammad Fahd | cuz that's what theyr looking for |
| Muhammad Fahd | \ |
| Muhammad Fahd | OK? |
| Muhammad Fahd | u need to be |
| Muhammad Fahd | cuz this isnt gonna work |

See also PSR, ¶18. FAHD also expressed frustration that another member of the scheme, N.L., aka “Wen,” aka “Winn,” had not followed his instructions to delete information, such as the malware and a surveillance tool they used called “FiddlerCap”:

| | |
|----------------------|--|
| Muhammad Fahd | they took marcs too |
| Muhammad Fahd | but marc deleted everything |
| Muhammad Fahd | Wen [N.L.] didn't |
| Kyra Evans | Oh wow |
| Kyra Evans | What did Wen [N.L.] have on there though . . . nothing right? |
| Muhammad Fahd | the app and fiddlershit |
| Kyra Evans | Fuck |

| | |
|----------------------|--|
| Muhammad Fahd | I told that nigga to go in for few mins |
| Muhammad Fahd | and delete it |
| Muhammad Fahd | but he didn't he wanted to wait for his shift |
| Kyra Evans | So they're gonna call him in fuuuck |
| Kyra Evans | Omg |
| Muhammad Fahd | but same thing deny deny deny |
| Muhammad Fahd | u need to relax tho |
| Kyra Evans | I feel like if anything happens it'll be because of Wen [N.L.] |
| Muhammad Fahd | yeah hes a bit weird |
| Muhammad Fahd | I told marc to school wen |
| Kyra Evans | Yea man |
| Kyra Evans | We will see |

See also PSR, ¶18. FAHD instructed Evans to make up an excuse for not going to an interview with Asset Protection, and told her to “deny everything”:

| | |
|----------------------|--|
| Muhammad Fahd | make up some excuse about having pregnancy issues |
| Muhammad Fahd | and go home |
| Muhammad Fahd | when are u leaving? |
| Kyra Evans | I'm not they are about to call me in |
| Muhammad Fahd | call u in for? |
| Muhammad Fahd | the same thing as marc? |
| Muhammad Fahd | deny everything |
| Muhammad Fahd | back? |
| Kyra Evans | Havent gone yet |

See also PSR, ¶18. FAHD also directed Evans to withdraw the proceeds she had received:

| | |
|----------------------|---|
| Muhammad Fahd | btw u need to start pulling all ur money out |
| Kyra Evans | Already started |
| Muhammad Fahd | in cash |
| Muhammad Fahd | not transfers |
| Muhammad Fahd | all of it |
| Muhammad Fahd | and then close the account |
| Kyra Evans | I started that yesterday |

Sapatin, Evans', and N.L.'s employment at AT&T ended, or was terminated, soon thereafter. PA, 9; PSR, ¶18. (Because Woods' involvement had not been discovered, Woods' employment was not terminated. PA, 9; PSR, ¶19.) Shortly later, Secret Service agents attempted to interview Sapatin, Evans, and N.L. After Sapatin informed FAHD that he had been contacted by law enforcement, FAHD instructed Sapatin not to say anything to law enforcement and to provide him with updates if law enforcement contacted him again. FAHD suspected that Evans had confessed and cooperated. FAHD told Sapatin that Evans would pay if she talked to law enforcement. *See* Plea Agreement, 10-11, *United States v. Sapatin*, CR18-00255RSL (Dkt. #9). He further told Sapatin that Evans had "fucked with" the wrong person. *Id.*

As the following data from FAHD's Google's accounted shows, the intervention by law enforcement prompted FAHD to search for ways to change his Google chat name, and to research whether he could be extradited from Pakistan to the United States:

| DATE | TIME | SEARCH |
|------------|--------------|--|
| | | Searched for how to change name in google account (https://www.google.com/search?q=how+to+change+name+in+google+account) |
| 10/26/2013 | 01:28:17 UTC | Searched for how to edit gchat name (https://www.google.com/search?q=how+to+edit+gchat+name) |
| 10/26/2013 | 01:40:24 UTC | Searched for united states jurisdiction (https://www.google.com/search?q=united+states+jurisdiction) |
| 10/30/2013 | 10:12:53 UTC | Visited http://en.wikipedia.org/wiki/Federal_jurisdiction_(United_States) |
| 10/30/2013 | 10:12:58 UTC | (http://en.wikipedia.org/wiki/Federal_jurisdiction_(United_States)) |
| 10/30/2013 | 10:13:52 UTC | Searched for united states jurisdiction in other countries (https://www.google.com/search?q=united+states+jurisdiction+in+other+countries) |
| 10/30/2013 | 10:13:56 UTC | Visited http://en.wikipedia.org/wiki/Jurisdiction (http://en.wikipedia.org/wiki/Jurisdiction) |
| 10/30/2013 | 10:14:01 UTC | Visited http://www.sitepoint.com/forums/showthread.php?523613-countries-that-the-U-S-doesn-t-have-jurisdiction (http://www.sitepoint.com/forums/showthread.php?523613-countries-that-the-U-S-doesn-t-have-jurisdiction) |
| 10/30/2013 | 10:18:44 UTC | Searched for extradition treaty (https://www.google.com/search?q=extradition+treaty) |
| 10/30/2013 | 10:18:51 UTC | Visited http://en.wikipedia.org/wiki/Extradition (http://en.wikipedia.org/wiki/Extradition) |
| 10/30/2013 | 10:18:53 UTC | Visited http://en.wikipedia.org/wiki/List_of_United_States_extradition_treaties (http://en.wikipedia.org/wiki/List_of_United_States_extradition_treaties) |
| 10/30/2013 | 10:22:07 UTC | Searched for extradition treaty with pakistan (https://www.google.com/search?q=extradition+treaty+with+pakistan) |
| 10/30/2013 | 10:26:00 UTC | Searched for any pakistanis from pakistan extradited to usa (https://www.google.com/search?q=any+pakistanis+from+pakistan+extradited+to+usa) |
| 10/30/2013 | 10:26:39 UTC | Visited http://dawn.com/news/787688/pakistani-facing-extradition-from-uk-to-us-over-hacking (http://dawn.com/news/787688/pakistani-facing-extradition-from-uk-to-us-over-hacking) |

D. Phase Two of the Scheme

Despite the intervention by law enforcement and AT&T, FAHD continued to develop ways to hack AT&T's system to unlock phones. In November 2014, FAHD

1 bragged to P.V. that he was going to hack AT&T so he could download the company's
2 entire network credential database:

| | | | |
|----|----------------|------|--|
| 3 | 11/5/2014 4:04 | Fahd | Fuck it. Ima tell jin [malware developer] to make me a |
| 4 | | | program to download the whole att nck db [nickname |
| 5 | | | database] |
| 6 | 11/5/2014 4:05 | Fahd | Even if in future shit goes down |
| 7 | | | |
| 8 | 11/5/2014 4:05 | P.V. | You sure |
| 9 | | | |
| 10 | 11/5/2014 4:05 | Fahd | We got it |
| 11 | | | |
| 12 | 11/5/2014 4:05 | P.V. | Don't want you to get in trouble |
| 13 | | | |
| 14 | 11/5/2014 4:05 | Fahd | Dont worry. I wont do it overnight. |
| 15 | | | |
| 16 | 11/5/2014 4:05 | Fahd | Ill make a work on a program for about a month or so |
| 17 | | | |
| 18 | 11/5/2014 4:06 | Fahd | Make it super stealth mission impossible type shit |
| 19 | | | |
| 20 | 11/5/2014 4:06 | Fahd | Which they wont detect at all. |
| 21 | | | |
| 22 | 11/5/2014 4:06 | Fahd | And then run it |
| 23 | | | |
| 24 | 11/5/2014 4:06 | P.V. | Oh cool |
| 25 | | | |
| 26 | 11/5/2014 4:06 | P.V. | Ya then sure |
| 27 | | | |
| 28 | 11/5/2014 4:06 | Fahd | This time im taking my time. |
| | | | |
| | 11/5/2014 4:06 | Fahd | If i do program shit |
| | | | |
| | 11/5/2014 4:07 | Fahd | Ima download that whole thing. |
| | | | |
| | 11/5/2014 4:07 | Fahd | And we will have that shit forever |

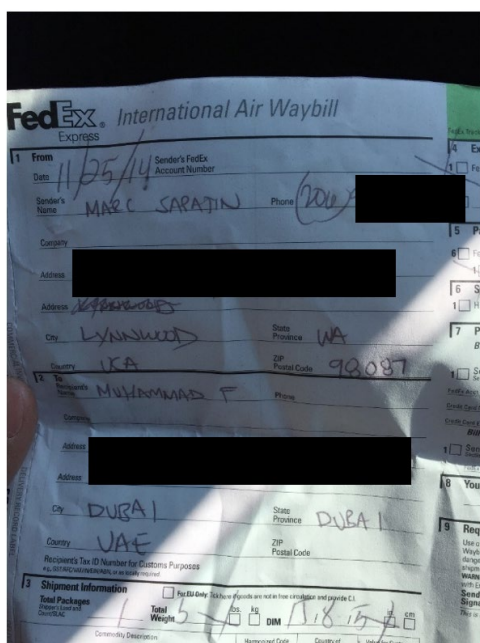
| | | |
|----------------|------|---|
| 11/5/2014 4:07 | Fahd | Lol |
| 11/5/2014 4:07 | P.V. | Your crazy man |
| 11/5/2014 4:07 | P.V. | But ya definitely worth it |
| 11/5/2014 4:07 | Fahd | I know. But im desperate. |
| 11/5/2014 4:07 | P.V. | Samsung alone is nice |
| 11/5/2014 4:07 | Fahd | For money |
| 11/5/2014 4:07 | Fahd | Yeah i know |
| 11/5/2014 4:08 | Fahd | I need to but a bigger house. Since its becoming small since my brothers kids. Wife. Mom dad. Sis. And me and my wife |
| 11/5/2014 4:08 | Fahd | So need a bigger house. |
| 11/5/2014 4:09 | Fahd | And thats gonna cost me around. 400 k plus |

In the fall of 2014, FAHD asked Sapatin to provide him with a list of people who still worked at AT&T and who might be willing to unlock phones illegally. FAHD and Sapatin ultimately decided to recruit Woods, who was still working at AT&T. PA, 9. FAHD contacted Woods to help him restart the scheme. PSR, ¶19. When Woods indicated that he did not wish to do so, FAHD threatened Woods and said that he would inform the police of Woods' participation in the earlier part of the scheme. Subsequently, Sapatin met with Woods and told him that FAHD was a powerful person and was watching Woods. At FAHD's direction, Sapatin made veiled threats to Woods about what would happen to Woods if he did not rejoin the scheme. *See* Plea Agreement, 8, *United States v. Woods*, CR18-00254RSL (Dkt. #9).

After coercing Woods to assist with the scheme, FAHD sent Sapatin a variety of hardware devices to provide to Woods. One type of device was a "key-grabber." This is a USB device that can be plugged into devices to capture keystrokes -- such as user

names and passwords -- that are entered through a keyboard. PA, 9. FAHD instructed Woods to plug the key-grabbers into the back of the workstations of over 20 customer service representatives at the Bothell call center when they were not at work. *See* PSR, ¶19. When the representatives returned to work and entered their network credentials, the key-grabbers would capture the credentials.

FAHD also sent a variety of internet routers for Woods to test on AT&T's computer system. *See* PSR, ¶¶19-20. The following photos from FAHD's iCloud account depict a router that FAHD sent to Sapatin in November 2014:



Working with a software developer, FAHD used the routers to attempt to breach AT&T's system and perform unlocks.

In approximately January 2015, FAHD successfully breached AT&T's system. He sent the following chats with former defendant Ghulam Jiwani (who was arrested in Hong Kong, but died before being extradited), announcing the breach:

| | | |
|----------------|--------|---------------------------|
| 1/15/2015 4:07 | Fahd | Congrats. We are in again |
| 1/15/2015 6:38 | Jiwani | What? |

| | | |
|-----------------------|-------------|----------------|
| 1/15/2015 6:38 | Jiwani | OMG |
| 1/15/2015 6:38 | Jiwani | Congrats |
| 1/17/2015 5:47 | Jiwani | Wow |
| 1/17/2015 5:49 | Fahd | Yup yup |

On August 10, 2015, FAHD paid for Sapatin to visit him in Dubai. Immediately after Sapatin arrived, FAHD asked Sapatin if he had come with anyone. In addition, FAHD had Sapatin lift up his shirt to check if he was wearing a wire. FAHD paid for Sapatin's airfare and hotel room, and gave him \$8,000. FAHD told Sapatin that he could not give him \$10,000 because of currency reporting requirements for transporting cash back to the United States. During the trip, they spent several days sightseeing and discussing the plan for continuing the unlocking scheme. Although FAHD prohibited Sapatin from taking pictures of him during the trip, FAHD took one picture, which the government later recovered through an email search warrant, of himself and Sapatin:



E. Threats and Intimidation

FAHD regularly took actions to intimidate members of the scheme. FAHD created the impression that he was someone who would take retribution against anyone who slighted him. For example, in the following communication with Evans, FAHD bragged about threatening to spend \$500,000 to hire someone to kill an ex-girlfriend who had dumped him:

Muhammad: im like i fly so far
Muhammad: to get dumped
Muhammad: wtf
me: gtfoh wow
Muhammad: yeah
me: smh
Muhammad: cried in my hotel for one week
Muhammad: then went back
Muhammad: tells me go jump off a cliff
Muhammad: and stop calling me
me: cold!
Muhammad: i was so mad
Muhammad: after the sadness
Muhammad: i was like ima empty my bank account , go hire a hit man
Muhammad: and im murder ur whole family
me: dayum serious type
Muhammad: i was like ima put a 500k hit on ur head
Muhammad: i was so mad
Muhammad: i was like its do or die
me: 0_0
me: crazzzzzy that's intense i would be mad too thogh
Muhammad: she's like starts beggin me
Muhammad: stop doing it
Muhammad: and stuff
Muhammad: i was like u had ur chance
Muhammad: its over
Muhammad: then i cooled off and let it go
Muhammad: she's scared shitless from me this day
Muhammad: tho
Muhammad: lol
me: hahahah i bet she is
Muhammad: oh btw
Muhammad: lil waynes been to my house
Muhammad: hahaha
Muhammad: random
Muhammad: lol
me: soooo jealous ...hate you
Muhammad: why u like him?
me: love like infatuated

1 The severe tone with which FAHD communicated with Woods is captured in two
2 recorded phone calls that are being submitted separately as Exhibits 9 and 10. In these
3 calls, FAHD tells Woods that he knows that Woods is lying to him, and abrasively
4 threatens to show Woods “what’s up” for betraying him.

5 **F. Money Laundering**

6 The scheme generated a large amount of proceeds. Between 2012 and 2017, Fahd
7 paid Sapatin at least \$441,500, Evans at least \$280,200, and Woods at least \$200,000.
8 FAHD typically made payments to Sapatin and Evans through P.V. and S.V. He
9 typically made the payments to Woods by having Jiwani deliver cash to Woods’
10 girlfriend, who would fly to Texas to receive the cash. In total, FAHD paid the AT&T
11 employees at least \$921,700 in bribes to participate in the scheme.

12 FAHD coached the insiders on how they should conceal the proceeds they
13 received. FAHD instructed Sapatin and Evans to set up fake businesses and bank
14 accounts for those businesses; to receive payments; and to create fictitious invoices for
15 every deposit made into the fake businesses’ bank accounts to create the appearance that
16 the money was payment for genuine services. Pursuant to these instructions, Sapatin and
17 Evans set up fake companies called Sapatin Enterprises and Jacinda Consulting, and bank
18 accounts in the name Marc C. Sapatin dba Sapatin Enterprises and Kyra J. Evans dba
19 Jacinda Consulting. At FAHD’s direction, Sapatin also issued fake invoices for services
20 that Sapatin Enterprises supposedly had provided to P.V.’s company, including the
21 following:
22
23
24
25
26
27
28

Sapatin Enterprises

INVOICE

P.O. Box [REDACTED]
Lynnwood, WA 98036
Phone: (512) [REDACTED]
Email: sapatinenterprises@gmail.com

DATE: 12/28/2012
INVOICE # 25
Customer ID 1

BILL TO

SwiftUnlocks
P.O. Box 99347
Anaheim, CA 92816
(916) 378-5123



| DESCRIPTION | TAXED | AMOUNT |
|--|-------|-------------|
| IT Services: | | \$12,000.00 |
| Ethical Hacking | | |
| Penetration Testing | | |
| Black-box Testing | | |
| White-box Testing | | |
| TCP/IP Review | | |
| Reverse Address Resolution Protocol (RARP) | | |
| Transport Layer Security (TLS) | | |
| Layer 2 Tunneling Protocol (L2TP) | | |
| Point-to-Point Protocol (PPP) | | |
| Serial Line Interface Protocol (SLIP) | | |
| | | |
| | | |
| | | |
| | | |

Subtotal \$ 12,000.00
Taxable \$ -
Tax rate 0.000%
Tax due \$ -
Other \$ -
TOTAL Due \$ 12,000.00

OTHER COMMENTS

1. Total payment due in 14 days
2. Please include the invoice number if method of payment is check
3. Wire transfers/cash deposits are acceptable methods of payment

Make all checks payable to
Sapatin Enterprises

G. FAHD Used the Proceeds to Live an Extravagant Lifestyle

The total amount of proceeds that FAHD obtained from the scheme is unknown due to the difficulty of obtaining overseas bank records. Existing records, including a spreadsheet maintained by FAHD, show that he received more than \$5.3 million in

1 | proceeds. At the time of his arrest, FAHD still had considerable proceeds and was living
2 | an extravagant lifestyle. Nevertheless, FAHD has refused to repatriate any of these
3 | proceeds for restitution.

4 | FAHD traveled regularly internationally, and typically flew first class or business
5 | class. For example, in the fourteen-month period from January 1, 2017, through
6 | February 2018, FAHD took 16 trips from Pakistan, each to between one and three foreign
7 | countries. Fahd usually stayed at luxurious hotels when he travelled, with a preference
8 | for the Ritz-Carlton.

9 | FAHD repeatedly bragged to members of the scheme about his luxury travel. For
10 | example, in an October 14, 2012 chat with Evans, FAHD bragged about staying at the
11 | Armani Hotel in Dubai at a cost of \$1,000 a night:

1 | Muhammad: btw i got another night on thursday to dubai again
2 | me: you go there a lot
3 | Muhammad: yeah i got investments
4 | Muhammad: there
5 | me: i seeeee
6 | Muhammad: youll see more lambos and ferraris and bentleys there then any other
7 | place
8 | Muhammad: i spent 15k on my last trip
9 | Muhammad: lol
10 | me: i got the list
11 | me: i want to see Dubai before i die
12 | Muhammad: yeah
13 | Muhammad: u should
14 | Muhammad: before that it was 25k
15 | Muhammad: lol
16 | Muhammad: its expensive
17 | Muhammad: but its worth it
18 | me: wow is it expensive or you just do expensive things?
19 | Muhammad: well , umm , i live large just saying
20 | me: hahah yea
21 | Muhammad: i always get a suite
22 | Muhammad: the armani cost me 1k a night
23 | Muhammad: plus services etc
24 | me: services huh
25 | me: lol
26 | Muhammad: room service
27 | Muhammad: lol
28 | me: yup
29 | me: ahahah
30 | me: Well that's whats up i wouldn't be spending like that but i DO want to go
31 | it looks beautiful
32 | me: list done
33 | Muhammad: well i had my gf with me
34 | Muhammad: so umm
35 | me: lol that explains a lot
36 | me: SHOPPING
37 | Muhammad: yeah
38 | Muhammad: but it was cool
39 | Muhammad: i got a watch

22 | Later in the conversation, FAHD went on to brag that the watch he purchased on the trip
23 | was an Audemars watch that cost around \$30,000.

24 | On January 17, 2013, FAHD bragged to Evans that he had hired the singer-
25 | songwriter Jay Sean to sing at his wedding for approximately \$100,000 to \$150,000:

Muhammad: i got jay sean to sing for my wedding , we talked yesterday a bit
Muhammad: 100k pretty crazy
me: Oh whaaaaat that's what s up!!!
Muhammad: plus hotel , limo and the setup is on me
Muhammad: 150 k probably for the whole thing
Muhammad: i hope its worth it

H. Fahd Throws Jiwani under the Proverbial Bus

In February 18, 2018, FAHD was arrested in Hong Kong. On May 8, 2018, during the course of his extradition proceedings, FAHD signed a statement in support of a non-refoulement claim, in which he sought to shift blame to Mr. Jiwani. Among other false claims, FAHD alleged that his life was “at risk” in Pakistan and that he was forced to work with Mr. Jiwani:

I was forced to work with the person I was arrested in Hong Kong. He belongs to a very influential family and have ties to the notorious MQM in Pakistan. **I was acting on his instructions out of fear and when we were arrested, he told me to take all the blame on myself.** I have been getting threats inside the prison. My family had to move out from Pakistan because they were getting threats from my co-accused’s family to take the blame. They sent police to my house to threat[en] my family in Pakistan. . . I fear that if I am sent to either Pakistan or [the] United States, my life will be in danger as both countries cannot provide me protection.

Signed Statement of Muhammad Fahd (Exh. 3) (emphasis added).

Shortly thereafter, on May 21, 2018, Mr. Jiwani died in Hong Kong custody. Nevertheless, FAHD and his lawyers continued to cast blame on Mr. Jiwani. For example, on July 3, 2018, FAHD’s attorneys submitted a filing in which they claimed that Mr. Jiwani’s family had forced FAHD’s family to flee Pakistan:

More recently, FAHD’s family has been receiving threats from JIWANI’s family in Pakistan. It is believed that JIWANI’s family sent the police to threaten FAHD’s family at their home in Pakistan. Consequently, the family moved out of Pakistan.

Submission for Bail on Behalf of Muhammad Fahd, 14.

1 **I. Loss Incurred by AT&T**

2 FAHD's actions caused immense loss to AT&T. As previously noted, when a
3 cellular telephone is unlocked prior to the expiration of a customer's contract, the
4 customer commonly moves to another carrier and ceases paying AT&T. As a result,
5 AT&T loses the unpaid balance of the price of the cellular phone (whether that was
6 reflected in a discount on the initial purchase recouped as part of monthly service charge,
7 or is the remaining balance on the installment contract for the telephone). *See* PA, 6;
8 PSR, ¶11. FAHD fraudulently unlocked millions of AT&T cellular telephones, and his
9 actions cost AT&T hundreds of millions of dollars.

10 AT&T's calculation of its loss is summarized in an Affidavit of Alfred B. Carter,
11 which is attached as Exhibit 1. Further details of the calculation are set forth in an AT&T
12 Executive Summary, which is marked as Exhibit 2.³ Carter recently retired as Director of
13 Asset Protection for an eight-State region that includes the State of Washington. As such
14 (prior to his retirement), Carter supervised other AT&T employees, including Abhijet
15 Railkar, who gathered relevant data, and an analyst, Ana Friedrichs, who spent the
16 equivalent of several months of full-time work analyzing data in the case.

17 As set forth in more detail in Carter's Affidavit, AT&T's analysis required two
18 steps: First, AT&T identified the number of illegal unlocks performed by the
19 conspirators. To do this, AT&T searched its databases to identify instances in which a
20 conspirator unlocked more than three cellular telephones in a minute. *See* Exhibit 1,
21 ¶¶15-16. Because a legitimate unlock, performed during a customer service call,
22 typically takes a substantial period of time, bulk unlocks of more than three per minute
23 necessarily were improper (and, often, the result of the use of malware). *See id.*, ¶16.

24 AT&T determined that, between October 12, 2012, and September 27, 2013,
25 Sapatin, Evans, and N.L. unlocked 1,802,871 cellular phones in batches of three or more
26

27 ³ The victim has marked this Exhibit as sensitive. Accordingly, the government will have this exhibit available at
28 the sentencing hearing in the event it is needed to respond to any defense argument regarding the loss issue.
Defense counsel has been provided a copy of this Exhibit in discovery.

1 per minute. (This number did not include the much smaller number of cellular phones
2 that the three unlocked at more regular intervals, presumably as part of their legitimate
3 duties.) AT&T also determined that between March 2, 2015, and August 9, 2017, the
4 user credentials of 16 different employees were used to unlock another 97,162 cellular
5 telephones in batches of three or more per minute. *See id.*, ¶18. This activity correlated
6 exactly with the period during which FAHD and Woods have admitted they were stealing
7 AT&T employee credentials – it did not happen in the months before or after that
8 conduct. *See id.* As a result, AT&T concluded that these unlocks also were the work of
9 the conspiracy. *See id.* In total, AT&T determined that FAHD was responsible for
10 fraudulently unlocking 1,900,134 cellular telephones.

11 Second, after determining the number of fraudulent unlocks, AT&T calculated the
12 lost revenue for each unlock. *See id.*, ¶¶19-24. Focusing on the 2012-2013 period
13 (which comprised roughly 95% of the unlocks), AT&T selected a random sample of
14 50,929 suspect unlocks. *See id.*, ¶19. AT&T concluded that it did not suffer a loss in the
15 case of half of those unlocks (most often because customers had completed their service
16 or installment contracts, and therefore had repaid AT&T the cost of their telephones).
17 *See id.* In the remaining cases, however, AT&T suffered a partial, or even total, loss.
18 *See id.*, ¶¶ 20-22. On average, AT&T determined that its loss was \$180.01 per phone for
19 the entire 50,929 sample. *See id.*, ¶23.

20 Multiplying the more-than-1.8 million fraudulent unlocks in 2012 and 2013 by the
21 \$180.01 loss per phone, AT&T determined that its loss during those years was
22 \$176,244,249.84. *See id.*, ¶23. Using a similar (but not identical) methodology, AT&T
23 determined that its loss during 2014-17 was an additional \$25,251,181.10. *See id.*, ¶24.
24 In total, for the entire period, AT&T's loss was \$201,497,430.94. *See id.*, ¶25.

25 It should be noted that AT&T's methodology is conservative and does not capture
26 the full loss caused by Fahd and his co-conspirators. This methodology focuses solely on
27 the "equipment cost" associated with the illegal unlocking. As a result, it reflects only
28 the remaining payments that the owners of the unlocked phones owed to AT&T on the

installment contracts they entered to buy the phones from AT&T, or the remaining amount of the subsidy that AT&T gave to the customers to purchase phones. The methodology does not include: (1) lost payments AT&T was entitled to receive under service contracts, (2) the cost of removing Fahd's malware from AT&T's computer systems, (3) or the significant resources that AT&T has had to expend to analyze its losses and respond to the government's requests for information in connection with this case.

III. PRESENTENCE REPORT

A. Guidelines Calculation

The government has no objection to the facts regarding the offense contained in the Presentence Report (PSR). In addition, the PSR appropriately calculates FAHD's Guidelines range as follows:

| Description | U.S.S.G. Provisions | Calculation |
|--|--|-------------|
| Base Offense Level | § 2X1.1(a) | 7 |
| Loss more than \$150,000,000 and less than \$250,000,000 | § 2B1.1(b)(1) / Application Note 3(F)(i) | +26 |
| A substantial part of a fraudulent scheme was committed from outside the United States/ sophisticated means. | § 2B1.1(b)(10) | +2 |
| Offense involved the trafficking of unauthorized access device | § 2B.1(b)(11) / Application Note 10(A) | +2 |
| Organizer or leader | § 3B1.1(a) | +4 |

| | | |
|---|------------------------------------|----|
| Obstruction or Impeding the Administration of Justice | § 3C1.1 / Application Note 4(D) | +2 |
| Acceptance of responsibility | § 3E1.1 | -3 |
| | TOTAL OFFENSE LEVEL | 40 |

As set forth in the Presentence Report, FAHD has a total offense level of 40 and a criminal history category of I, which normally would result in an advisory sentencing range of 292-365 months. *See* PSR, ¶¶ 26-39. However, in this case, the Guidelines range of imprisonment exceeds the statutory maximum sentence of 20 years. Accordingly, FAHD's advisory Guidelines range is 20 years, pursuant to USSG § 5G1.1.

B. Responses to the Defendant's Anticipated Objections

The defense raised several objections to the PSR, and the government incorporates by reference the addendum to the PSR which fully addresses each of those objections. However, in anticipation of arguments that the defense will raise at sentencing, the government addresses two objections below.

1. Leadership Enhancement

The defense incorrectly contends that FAHD was not the true leader of the criminal enterprise. This contention is at squarely at odds with stipulations in the plea agreement and PSR that FAHD (1) recruited and controlled the AT&T insiders; (2) instructed Sapatin and Evans to set up fake businesses to launder proceeds; and (3) developed the malware and hacking tools to compromise AT&T's computer system. Moreover, Sapatin, Evans, and Woods all have identified FAHD as the singular leader of the enterprise. Accordingly, the defense's attempt to shift responsibility to other parties should be rejected.

1 **2. Loss Amount**

2 The PSR correctly recommends that the Court apply a 26-level upward
3 adjustment, based upon a loss of more than \$150,000,000. *See* U.S.S.G.
4 § 2B1.1(b)(1)(N). The Court should do so, for any of several reasons:

5 *i. AT&T's Loss Calculation*

6 As noted and described in Part II.I above, AT&T has calculated that its losses are
7 \$201,497,430.94, an amount that exceeds \$150,000,000. This calculation is supported by
8 the sworn Affidavit of Alfred Carter. *See* Exh. 1. This Affidavit exhaustively documents
9 how the illegal unlocking caused by FAHD and the employees whom he bribed at AT&T
10 resulted in the loss of that much revenue from the sale of cellular telephones.

11 It is true that FAHD and the bribed employees are not the only persons responsible
12 for this loss – the customers who paid to have their cellular telephones unlocked also bear
13 some responsibility. But, AT&T would not have suffered these losses unless FAHD and
14 his co-conspirators fraudulently unlocked the customers' cellular telephones, because the
15 customers could not have walked away from their agreements to pay for their telephones
16 and switched service to other companies absent this unlocking. As a result, this loss
17 clearly falls within the Sentencing Guidelines' definition of loss, that is, "the reasonably
18 foreseeable pecuniary harm that resulted from the offense." *See* U.S.S.G. § 2B1.1,
19 Application Note 3(A)(i).

20 The defense takes issue with AT&T's calculation of the loss amount but offers no
21 alternative calculation other than to claim – without legal or factual support – that the loss
22 amount should be limited to \$1.8 million. The defense's position is peculiar, because
23 FAHD has stipulated to the fact that the illegal unlocking allowed customers to stop
24 making payments on their service and/or installments contracts, thereby causing AT&T
25 to lose the outstanding portion of the payment due for the equipment cost of the phone.
26
27
28

1 | See PA, 6; PSR, ¶11. In light of this stipulation, there is no reason not to recognize the
2 | full magnitude of the loss caused to the victim in this case.⁴

3 | The defense's objection appears primarily to be a reaction to how high the loss
4 | number is. However, the loss number is so high because FAHD's seven-year hacking
5 | scheme unlocked at least *1.9 million* phones, not because the victim's loss calculation
6 | overstated the damage FAHD caused. Indeed, AT&T's loss calculation was exceedingly
7 | conservative. Among other things, AT&T's calculation includes only the equipment cost
8 | of the phones – namely the remaining cost of the phone for the customers who walked
9 | away after their phones were unlocked. AT&T's calculation does not include the lost
10 | revenue it was entitled to receive pursuant to the customers' service contracts, even
11 | though AT&T was entitled to do so. See Carter Affidavit, ¶19 n. 3 (Exh. 1); cf. *United*
12 | *States v. Ali*, 620 F.3d 1062, 1067-68 (9th Cir. 2010) (finding that depriving a victim of
13 | future revenue it was contractually entitled to receive constituted a fraud under the wire
14 | fraud statute). Nor does AT&T's loss calculation include 3,229 hours its employees
15 | spent investigating and remediating the harm that FAHD caused. See Victim Impact
16 | Statement.

17 | Moreover, as discussed in Section II.I, *supra*, AT&T's loss calculation was
18 | painstakingly precise. An analyst – who defense counsel had an opportunity to interview
19 | – spent *months* going through a random sample of 50,929 accounts that were illegally
20 | unlocked. That analyst carefully removed from the loss calculation all the accounts for
21 | which it could be claimed that AT&T did not suffer an equipment cost loss. Given that
22 | AT&T's precise and conservative loss calculation is detailed in Exhibits 1 and 2, and
23 |
24 |

25 | ⁴ Notably, FAHD has had every chance to challenge this calculation or to offer an alternative loss methodology.
26 | First, AT&T has permitted defense counsel to conduct interviews, and counsel has in fact conducted interviews, of
27 | each of Abhijet Railkar, Ana Friedrichs, and Alfred Carter. Second, the government indicated to defense counsel
28 | that it intended to rely upon the Affidavit of Alfred Carter, but that it would work with AT&T to facilitate the
attendance of these witnesses at FAHD's sentencing, in the event that FAHD's counsel wished to conduct cross
examination of any of these individuals. FAHD's counsel declined that offer. As a result, FAHD's counsel have
been offered, and declined, an opportunity to conduct cross examination of any of these individuals, and the Court
properly can rely on Carter's sworn Affidavit.

1 given that defense counsel had the opportunity to interview the AT&T employees who
2 performed the calculation, the defense cannot meaningfully challenge the calculation by
3 simply claiming the calculation is too high.

4 *ii. Application Note 3(F)(i)*

5 Even if the Court were inclined to question AT&T's loss calculation, the
6 commentary to § 2B1.1 results in exactly the same 26-level adjustment for loss.

7 Application Note 3(F)(i) to § 2B1.1⁵ provides that

8 In a case involving any counterfeit access device or
9 unauthorized access device, loss includes any unauthorized
10 charges made with the counterfeit access device or
11 unauthorized access device and shall be not less than \$500
12 per access device. However, if the unauthorized access
13 device is a means of telecommunications access that
14 identifies a specific telecommunications instrument or
15 telecommunications account (including an electronic serial
16 number/mobile identification number (ESN/MIN) pair), and
17 that means was only possessed, and not used, during the
18 commission of the offense, loss shall be not less than \$100
19 per unused means. For purposes of this subdivision,
20 **“counterfeit access device”** and **“unauthorized access
21 device”** have the meaning given those terms in Application
22 Note 10(A).

19 U.S.S.G. § 2B1.1, Application Note 3(F)(i).

20 Application Note 10(A), in turn, defines “counterfeit access device” to have the
21 meaning set forth in 18 U.S.C. § 1029(e)(2) – that is, “any access device that is
22 counterfeit, fictitious, altered, or forged.” *See also* 18 U.S.C. § 1029(e)(1) (defining
23 access device to “mean any card, plate, code, account number, electronic serial number,
24

25
26 ⁵ The Ninth Circuit has affirmed the application of Application Note 3(F)(i) to calculate loss amounts in numerous
27 cases. *See, e.g., United States v. Truong*, 587 F.3d 1049, 1050 (9th Cir. 2009). Earlier this year, the Sixth Circuit
28 issued an opinion rejecting the validity of Application Note 3(F)(i), on the theory that this note added to, rather than
interpreted, § 2B1.1. Presumably as a result, the Ninth Circuit recently ordered the parties in one case to brief the
validity of Application Note 3(F)(i). *United States v. Kirilyuk*, 2021 U.S. App. LEXIS 22118, No. 19-10447, Order
(9th Cir. Jul. 26, 2021).

1 mobile identification number, personal identification number, or other
2 telecommunications service, equipment or instrument identifier . . . that can be used . . .
3 to obtain money, goods, services, or any other thing of value.”). Application Note 10(A)
4 further expressly provides that the term “counterfeit access device” “includes a
5 telecommunications instrument that has been modified or altered to obtain unauthorized
6 use of telecommunications service.” U.S.S.G. § 2B1.1, Application Note 10.

7 In this case, the IMEIs that FAHD possessed, and that he submitted to AT&T to
8 unlock cellular telephones, were access devices because they were “mobile identification
9 numbers . . . that can be used . . . to obtain services,” 18 U.S.C. § 1029(e)(1), namely
10 telephone service. They were counterfeit, because they had been “altered” “to obtain
11 unauthorized use of telecommunications service.” 18 U.S.C. § 1029(e)(2); U.S.S.G.
12 § 2B1.1 Application Note 10(A). FAHD possessed, but did not use, the access devices.
13 Therefore, his loss is at least \$100 per access device. U.S.S.G. § 2B1.1, Application Note
14 3(F)(i). Based upon the more-than-1.9-million telephones that Fahd unlocked, his loss
15 amount is at least \$190,000,000, which results in the same 26-level upward adjustment as
16 AT&T’s calculation.

17 And, even if the Court were to discount AT&T’s conclusion that FAHD was
18 responsible for more than 1.9 million unlocks, FAHD admitted in his plea agreement, that
19 he was responsible for unlocking 1,117,503 phones during the three months between June
20 27, 2013, and September 27, 2013, plus additional “substantial numbers of unlocks”
21 during the much-longer periods between August 2012 and June 26, 2013, and between
22 late 2014 and September 2017. *See* PA, ¶ 8. Thus, FAHD’s plea agreement itself
23 supports a conclusion that Fahd unlocked more than 1.5 million telephones, and he
24 therefore is responsible for a loss of more than \$150 million pursuant to Application Note
25 3(F)(i), and should receive a 26-level adjustment without any reference to AT&T’s loss
26 calculation.

1 *iii. Estimation of Loss*

2 Even in the absence of AT&T's loss calculation and Application 3(F)(i), the
3 record in this case supports the conclusion that AT&T's loss exceeded \$150 million, and
4 that FAHD should receive a 26-level adjustment for loss. The Sentencing Guidelines do
5 not require a precise calculation of loss. Rather "[t]he court need only make a reasonable
6 estimate of the loss." U.S.S.G. § 2B1.1, Application Note 3C. In doing so, a court may
7 consider factors such as "[t]he fair market value of the property unlawfully taken, copied,
8 or destroyed" and "[t]he approximate number of victims multiplied by the average loss to
9 each victim." *Id.*, Application Note 3(C)(i), (iv).

10 Here, FAHD has admitted in his plea agreement that cellular telephones "cost
11 hundreds of dollars." *See* PA, ¶ 8. He has admitted that "[w]hen phones were unlocked
12 and transferred to other networks, some customers stopped making payments on their
13 service and/or installment contracts. As a result, AT&T lost the outstanding portion of
14 the payment due for the initial price of the phone." *See id.* And, he has admitted being
15 responsible for improperly unlocking 1,117,503 phones during a three-month window,
16 plus "substantial numbers" of additional phones during periods totaling more than three
17 additional years. *See id.*

18 These facts by themselves are sufficient for the Court to estimate the loss caused
19 by FAHD's misconduct for purposes of calculating FAHD's offense level. Assuming an
20 average loss of \$134.22 per cellular phone (a small percentage of the cost of phones that
21 that FAHD has admitted), and multiplying by 1,117,503 (the minimum number of phones
22 unlocked by FAHD's own admission) results in a loss of \$150 million to AT&T.
23 Because both this loss amount and the number of phones are conservative, the Court can
24 and should find that FAHD's admissions alone are sufficient to support the conclusion
25 that FAHD's conduct caused AT&T more than \$150 million in losses, and therefore
26 FAHD's offense level should be increased by 26 levels as a result.

IV. SENTENCING RECOMMENDATION

The United States recommends (1) a 15-year custodial sentence with credit for time served since FAHD's arrest in Hong Kong on February 4, 2018; (2) a three-year term of supervised release; (3) a restitution judgment in the amount of \$200,620,698; (4) a forfeiture judgment in the amount of \$5,338,430; and (5) a special assessment in the amount of \$100. This Guidelines sentence is sufficient, but not greater than necessary, and is justified by a balancing of the factors set forth in Title 18, United States Code, Section 3553(a).

As the Ninth Circuit and the Supreme Court have explained, the Sentencing Guidelines are "the 'starting point and the initial benchmark' . . . and are to be kept in mind throughout the process." *United States v. Carty*, 520 F.3d 984, 996 (9th Cir. 2008) (internal citations omitted). Section 3553(a) sets forth factors for the Court to consider alongside the advisory Guidelines range. The United States submits that the recommended sentence is appropriate, particularly in light of "the nature and circumstances of the offense," "the history and characteristics of the defendant," and the need for the sentence "to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense," "to afford adequate deterrence to criminal conduct," and "to avoid unwarranted sentence disparities." 18 U.S.C. §§ 3553(a)(1), (a)(2), and (a)(6).

A. Sentencing Factors

1. The Nature and Circumstances of the Offense

The nature and circumstances of FAHD's offense are extremely serious. For seven years, FAHD was the mastermind behind a brazen hacking scheme that caused massive harm to a U.S. victim. He maintained his control over his underlings through bribery, intimidation, and outright threats. Not only did FAHD cause over 200 million dollars in damage, he also irrevocably harmed the young people he exploited and manipulated.

1 Each of the following aggravating factors related to the nature and circumstance of
2 FAHD's hacking scheme weighs heavily in support of a 15-year sentence:

3 a. *FAHD was the Mastermind and Driving Force Behind the*
4 *Sophisticated Hacking Scheme*

5 Without Muhammad FAHD, there would have been no hacking scheme: he came
6 up with the idea of hacking AT&T; he recruited and managed the AT&T insiders; he
7 hired hackers to develop ways to infiltrate AT&T's unlocking system to perform bulk
8 unlocks; and he restarted the scheme despite an earlier intervention by law enforcement
9 and AT&T. FAHD did all things because he was the undeniable, top-level leader of the
10 seven-year criminal enterprise.

11 This was not a simple hacking scheme. Day in and day out, FAHD spent seven
12 years working on ways to repeatedly infiltrate AT&T's computer systems. It took him
13 hundreds of thousands of dollars to bribe the young AT&T employees to give him access
14 to their employer's computer systems. Yet, even more resources were required to
15 develop the custom software and hardware tools FAHD deployed to conduct illegal
16 unlocks on a large scale. FAHD's hacking scheme was so large, it essentially functioned
17 as an enterprise with millions of dollars of illegal revenue and scores of customers who
18 sought to illegally unlock over 1.9 million phones.

19 FAHD was successful because he was ambitious and relentless. As FAHD
20 bragged in the communication in Section II.D, *supra*, his goal was to completely
21 compromise AT&T's system so he could gain all the network credentials he needed to
22 perform large amounts of illegal unlocks. It is one thing to launch a single attack against
23 a company's security. It is quite a different thing to spend over seven years seeking to
24 compromise a company's security. Simply put, the level of sophistication and
25 persistence that FAHD displayed is rarely seen and underscores that he poses a unique
26 and ongoing threat to victims.

1 b. *FAHD Repeatedly Engaged in Exploitation, Intimidation, and*
2 *Obstruction of Justice*

3 FAHD went to great lengths to portray himself as a gangster-type leader of the
4 scheme. FAHD masterfully targeted young, impressionable people who he knew would
5 be susceptible to his larger-than-life persona and his repeated promises of easy money.
6 He bragged about his wealth and luxurious lifestyle, making sure to emphasize the
7 expensive items he bought (e.g., cars, watches) and the extravagant hotels rooms he
8 frequented. And, he carefully manipulated them by gradually increasing the bribes they
9 received to the point that he knew that they would obey him blindly because he was
10 giving them so much more money than they could earn legitimately.

11 Just as FAHD portrayed himself as a successful criminal who could offer his
12 underlings easy money, he also portrayed himself as someone who would inflict
13 retribution for disloyalty. Among other things, he used tough language and racial slurs to
14 give the impression that he was from the “street” and would seek street-style vengeance
15 on anyone who crossed him. It was no coincidence that FAHD bragged to Evans that he
16 had tormented his ex-girlfriend for dumping him and had threatened the ex-girlfriend that
17 he would put a \$500,000 “hit” on her head. Fortunately, the severe tone with which he
18 dealt with his underlings is captured in the two recorded calls with Woods in which
19 FAHD abrasively confronts Woods about his suspicions about Woods. FAHD ends the
20 last conversation with the following threat: “If this is how its gonna be, then you’ll find
21 out how it’s gonna be And, about everything else, you’ll know what’s up.” Although
22 FAHD’s speech and conduct may seem comic in retrospect, members of the scheme,
23 including DeVaughn Woods (who is 6’3”, and almost twice as large as FAHD), were
24 acutely afraid of FAHD. Woods, for example, had the reasonable fear that FAHD would
25 take retribution against him and his family for being caught. *See Sentencing*
26 *Memorandum of Defendant, at 6-7, United States v. Woods, CR18-254RSL (Dkt. # 41)*
27 *(describing FAHD’s various threats).*
28

1 Consistent with his gangster persona, FAHD mentored his underlings on how to
2 be better criminals. He instructed them to set up fake companies to launder the large
3 amount of proceeds he gave them. And, he instructed them to hide their wealth. It
4 should be no surprise that FAHD also coached his underlings on how to obstruct justice.
5 When AT&T and law enforcement first intervened in 2013, FAHD demanded that his
6 underlings deny everything and destroy evidence. In the conversation between FAHD
7 and Evans contained in Section II.C.3, *supra*, FAHD expressed his anger when N.L. did
8 not follow his instruction to delete the malware and surveillance tools FAHD deployed,
9 and stated “I told that nigga to go in for few mins . . . and delete it. . . but he didn’t [,] he
10 wanted to wait for his shift.” FAHD also warned Evans to do a better job when
11 confronted by investigators and instructed her to “deny deny deny.”

12 c. *FAHD Restarted the Hacking Scheme Despite an Intervention by*
13 *Law Enforcement.*

14 Despite the intervention by AT&T and law enforcement and the fact that Sapatin
15 and Evans lost their jobs, FAHD was completely undeterred. FAHD understood that
16 there very well could be criminal consequences both for his underlings and himself. It is
17 for this reason that, in 2013, FAHD ran a number of searches on the risk he faced of
18 being extradited to the United states. *See* Section II.C.3, *supra*. Nevertheless, FAHD
19 redoubled his efforts to breach AT&T so he could resume his illegal unlocking enterprise.

20 FAHD did not hesitate to exacerbate the damage he had caused to the young
21 people he exploited, and quickly brought Sapatin back into the scheme so that FAHD and
22 Sapatin could extort Woods into doing FAHD’s bidding again. It is unusual to have the
23 leader of a cybercriminal enterprise strike again at a prior victim. It is even more unusual
24 to have the leader of such an enterprise be so willing to put members of his enterprise
25 repeatedly into harm’s way. The fact that FAHD did both of these things is a testament
26 not only to his remarkable greed but also his callousness as a leader.

1 d. *FAHD Feels Little Remorse for the Massive Harm He Caused*

2 There should be no question that FAHD caused massive harm to both AT&T and
3 the people he exploited. Yet, at every juncture, FAHD has sought to minimize and
4 downplay the harm he caused, either through his own statements, or through his
5 attorneys. FAHD had no compunction about compounding the harm he caused to Sapatin
6 and Woods when he brought them back into the hacking scheme. FAHD expressed no
7 regret that Evans, Sapatin, Woods now have felony convictions and face massive
8 restitution judgements. Even worse, perhaps, FAHD had no shame when he betrayed
9 Jiwani in Hong Kong to save his own skin. Instead of feeling remorse for being
10 responsible for his close friend's arrest and incarceration, FAHD sought to capitalize on
11 Jiwani's vulnerability, even after Jiwani's unfortunate death in Hong Kong custody.

12 Similarly, FAHD has had no remorse for the economic harm he caused. The
13 impact of FAHD's crime on AT&T was undeniably massive. FAHD illegally unlocked
14 at least *1.9 million* phones. It is not surprising that the equipment loss associated with
15 such a massive number of illegal unlocks amounted to over *\$200 million* in damage. The
16 loss to AT&T should not be discounted as mere loss to a large corporation. AT&T, like
17 other corporations, incorporates fraud losses in setting prices for its product and services.
18 AT&T customers across America each ultimately bore a small portion of this loss in the
19 form of higher cellular telephone prices. Moreover, the loss in profitability was felt by
20 AT&T's shareholders, many of whom are pension funds.

21 The defense attempts to sidestep the scope and the magnitude of the economic
22 harm caused FAHD's offense by saying that the loss amount should be based on FAHD's
23 financial gain and, even then, the defense asks the Court to find that FAHD made only
24 \$1.8 million when FAHD's own records show that he made over \$5 million. The defense
25 further suggests that both the conservative loss calculation provided by AT&T and the
26 presumed minimum loss under the Sentencing Guidelines are disproportionate to the
27 actual harm that FAHD caused. However, a sophisticated cybercriminal like FAHD
28

1 should not be permitted to raise disproportionality as a shield for at least two central
2 reasons.

3 ***First***, the asymmetry between the relatively limited investment of resources by
4 cybercriminals and the enormous harm they cause is exactly what makes cybercrime so
5 alluring. Cybercriminals like FAHD pose such a great threat because they use their
6 specialized skills and training to amplify the reach and impact of their criminal activity.
7 Instead of having to physically rob thousands of AT&T stores to obtain unlocked cellular
8 phones, FAHD was able to use his custom malware and hacking tools to perform *millions*
9 of illegal unlocks through a single AT&T call center, all from the comfort and safety of
10 his keyboard in Pakistan. Consequently, FAHD cannot fairly invoke disproportionality
11 when he made a deliberate decision to leverage his technological expertise to carry out
12 his criminal activity on a massive scale.

13 ***Second***, and relatedly, the asymmetrical harm caused by FAHD's offense was the
14 foreseeable and intended consequence. This is not a case where a defendant takes a
15 simple action that cascades into a series of unpredictable events. To the contrary, FAHD
16 knew exactly what he was doing and the harm it would cause. Namely, FAHD intended
17 to unlock the phones so his customers could walk away from their contracts with AT&T.
18 Because this was the intended result of his relentless attacks on AT&T's security, FAHD
19 cannot now claim to be a victim of his own success in helping to accomplish this goal.

20 **2. The Defendant's History and Characteristics**

21 FAHD's history and characteristics indicate that a 15-year sentence would be
22 appropriate. Very few positive things can be said about FAHD's history and
23 characteristics. The evidence demonstrates that FAHD was relentlessly driven by his
24 greed and repeatedly displayed a complete disregard for the people he exploited. FAHD
25 repeatedly has shown a tendency to exploit, intimidate, and obstruct. And, he was
26 particularly ruthless in the manner he dealt with his former friend Jiwani in Hong Kong.

27 FAHD's conduct after his extradition to the United States also does not reflect
28 favorably on his history and characteristics. FAHD came from a well-off family that ran

1 multiple businesses. In addition, FAHD made an enormous amount of money from the
2 hacking scheme. Although FAHD spent a great deal of money to fund his extravagant
3 lifestyle, he clearly still had access to vast financial resources at the time of his arrest in
4 Hong Kong.

5 In particular, FAHD's extensive international travel provides insight into how
6 much money he had before his arrest. According to airline records, in the fourteen-month
7 period from January 1, 2017 through February 2018, FAHD took at least 16 trips from
8 Pakistan, each to between one and three foreign countries. The vast majority of the trips
9 for which information is available involved first class or business class tickets. During
10 these trips, FAHD often stayed at luxurious hotels. For example, hotel records show that
11 he stayed at Ritz-Carlton hotels, in Doha, Qatar, Bangkok, Thailand, and Tokyo, Japan.
12 Needless to say, this is not how a poor, disadvantaged individual travels.

13 Even after FAHD's arrest, he continued to show that he has access to great
14 financial resources. FAHD relocated his entire family to Hong Kong, hired a high-
15 powered legal team, and offered to put up a large bail amount while contesting
16 extradition. And, after his extradition to the United States, his family continued to fund
17 multiple legal teams.

18 Despite amassing a large amount of illegal proceeds and having great financial
19 resources, FAHD has made no meaningful effort to bring funds back into the United
20 States to pay restitution. As required by his plea agreement, FAHD sat for an interview
21 regarding his finances and his ability to pay restitution. That interview is captured, in
22 part, in Exhibit 4, which is a summary memorandum of that interview. Although FAHD
23 purported to cooperate, the substance of the interview shows that FAHD has actually
24 decided to stonewall and to keep whatever money he has, rather than actually beginning
25 to compensate his victim.

26 During the interview, FAHD claimed near-complete amnesia regarding his past
27 finances. He denied virtually every aspect of the luxurious lifestyle he lived, including
28

1 his possession of expensive watches and cars. FAHD even claimed he could not
2 remember the details of his extensive travel:

3 During the aforementioned 10/14/2012 chat conversation, Fahd told a co-
4 conspirator he had stayed at the Armani Hotel at a cost of approximately
5 \$1,000 per night. He also told the co-conspirator he had spent
6 approximately \$15,000 during one of his trips, and approximately \$25,000
7 during another trip. When asked if he had ever stayed at the Armani Hotel,
8 Fahd said he might have stayed there, but didn't know. When asked about
approximately 16 trips the government's investigation showed he took
to/from Pakistan from 2017 to 2018, he said he could not recall those trips .

9 ...

Exh. 4, 3.

10 In addition, FAHD expressed no willingness to assist in identifying his assets. He
11 claimed not to recall how much money he had in an account at Emirates NBD, a bank
12 that previously was his principal account. *Id.* He claimed he could not even estimate
13 how much money ever was in the account. *Id.* Rather than provide any helpful
14 information about any of his assets, he claimed simply that "he d[id]n't know what
15 happened to the money he made unlocking phones." *Id.* at 2.

16 Predictably, FAHD declined to take any proactive steps to assist in returning funds
17 to the United States:

18 When asked what steps he was willing to take in order to make contact with
19 his financial institutions and arrange a transfer of funds to make payments
20 towards his restitution, Fahd said he didn't know. When then asked if he
21 was willing to help with this process, Fahd said he didn't know. When
22 asked if he was willing to solicit assistance from his family members or
23 friends with making contact with his financial institutions or the Pakistani
24 tax authorities, Fahd said he didn't know. He said his parents are elderly
25 and unable to assist. Fahd said the banks would not assist with this process
and repeated that Pakistani tax authorities may have seized his money. He
later changed his answer and said the Pakistani government definitely
seized his money

26 *Id.* at 2.

27 FAHD's apparent amnesia is laughable. In short, it is clear that FAHD has
28 decided to hide the proceeds of his crime, for his own benefit, when he is released. This

1 is not the conduct of an individual who has accepted responsibility. Rather, it is the
2 conduct of an unrepentant criminal who has decided to keep the proceeds of his crime,
3 rather than begin to provide restitution to his victim (and of one who presumably will
4 resume his chosen profession once he is released from U.S. custody). The government
5 cannot force FAHD to surrender the proceeds of his crime, which are hidden overseas,
6 but one consequence of FAHD's refusal to do so should be that FAHD receives a
7 sentence that reflects the choice that FAHD has made – the 15-year sentence the
8 government is recommending – rather than a lesser sentence that acquiesces to FAHD's
9 continued refusal to repay money obtained by his crime.

10 **3. The Need for the Sentence to Reflect the Seriousness of the Offense, to**
11 **Promote Respect for the Law, and to Provide Just Punishment**

12 These factors weigh strongly in favor of a judgment that imposes a lengthy term of
13 incarceration. Crimes like those committed by FAHD are a serious threat to the viability
14 of businesses everywhere, as well as to the security of their customers. A 15-year
15 custodial sentence would send a message that there are harsh consequences for launching
16 repeated attacks against U.S. businesses and for exploiting impressionable young people
17 who work at those companies.

18 The need to promote respect for laws that prohibit cybercrime is particularly high
19 given the major increase in attacks against U.S. interests that are launched by foreign
20 actors. It is rare that the top-level leader of a sophisticated cybercriminal organization is
21 identified, arrested, and extradited for prosecution in the United States. Too often,
22 international cybercriminals can conceal their identities or hide in countries in which they
23 are beyond the reach of law enforcement. Accordingly, cases such as this one present a
24 rare opportunity to demonstrate that not only can law enforcement identify and arrest
25 leaders of sophisticated cybercriminal enterprises, but also that such cybercriminals face
26 harsh consequences for attacking U.S. businesses and customers.

27 Finally, no discussion of these factors would be complete without additional
28 mention of the enormous harm that FAHD caused. As discussed above, not only has

1 FAHD caused over \$200 million in losses, he has left an indelible mark on the young
2 people he manipulated. A 15-year sentence is needed to provide just punishment and to
3 vindicate the interests of these victims.

4 **4. The Need to Protect the Public from Further Crimes from FAHD**

5 FAHD's contempt for his obligation to pay restitution under the plea agreement
6 and his unwillingness to fully accept responsibility for the full magnitude of the harm he
7 caused indicate that he poses an extremely high risk of recidivism. Indeed, FAHD's past
8 history indicates that he has no compunction with resuming his criminal even after law
9 enforcement has intervened. The only lesson that FAHD likely has learned from his
10 arrest and incarceration is that he needs to be more careful about his travel in the future
11 after he resumes his cybercriminal activity. Therefore, a lengthy sentence is needed to
12 protect the public from FAHD.

13 **5. The Need to Afford Adequate Deterrence to Criminal Conduct**

14 High rewards and a relatively low risk of detection are basic features of modern
15 cybercrime. However, appropriately severe sentences can impact the cost-benefit
16 analysis of would-be cybercriminals. Computer hackers are among the most
17 sophisticated criminals in the world and are known to closely monitor U.S. authorities'
18 response to cybercrime and plan accordingly. Achieving general deterrence in this area,
19 therefore, appears somewhat promising. *See United States v. Martin*, 455 F.3d 1227,
20 1240 (11th Cir. 2006) (because "economic and fraud-based crime are more rational, cool,
21 and calculated than sudden crimes of passion or opportunity, these crimes are prime
22 candidates for general deterrence").

23 This case demonstrates that there is an acute need to impose a sentence that deters
24 others from joining cybercriminal organizations. Criminal enterprises such as FAHD's
25 illegal unlocking enterprise rely on the ability to recruit technologically skilled
26 individuals and corporate insiders. A fifteen-year sentence will put potential recruits on
27 notice that engaging in cybercrime will subject them to significant prison sentences that
28 are commensurate with the harm they cause. Giving the leader of a cybercriminal

1 enterprise a lengthy jail sentence will convincingly show at least some would-be
2 cybercriminals that the cost of doing business is too high.

3 **6. The Need to Avoid Unwarranted Sentence Disparities**

4 Cybercrime takes many forms, and it is difficult to compare cybercriminal
5 schemes that utilize different methodologies and that impact different groups of victims.
6 For this reason, it is difficult to compare sentences imposed on defendants who
7 participated in different cybercriminal enterprises. Nevertheless, there are several cases
8 from the Western District of Washington that provide important reference points.

9 In the first case, *United States v. Schrooten*, CR12-085RSM, Judge Martinez
10 sentenced a prominent hacker and payment card thief to 12 years pursuant to a
11 Rule 11(c)(1)(C) plea agreement. Although Schrooten's carding ring was considered
12 substantial at the time, he had in his possession only 100,000 stolen payment card
13 numbers.

14 In the second case, *United States v. Roman Seleznev*, CR11-70RAJ, Judge Jones
15 sentenced the leader of an extensive payment card trafficking ring to 27 years after he
16 was convicted at trial. Seleznev was held responsible for 2.9 million stolen payment
17 cards that were found in his possession. There were many aggravating factors in
18 Seleznev's case including his leadership role, the millions in proceeds he received, his
19 extensive efforts to obstruct justice, and evidence that he had stolen many more payment
20 cards.

21 In the third case, *United States v. Hladyr*, CR17-0027RSM, Judge Martinez
22 sentenced a high-level manager of the cybercriminal enterprise known as FIN7 after the
23 hacker pleaded guilty to one count of conspiracy to commit wire fraud and one count of
24 conspiracy to commit computer hacking. Hladyr made only approximately \$100,000 in
25 proceeds for his involvement in the enterprise and lived a frugal life. However, the loss
26 caused by FIN7 was astronomical.

27 Of the three cases, the *Seleznev* case is the most pertinent. Like Selznev, FAHD
28 was the top-level leader of his criminal enterprise and received millions in proceeds.

1 Furthermore, both men took steps to obstruct justice and pose a high risk of recidivism.
2 Accordingly, a 15-year sentence would be entirely consistent with the sentence imposed
3 in *Seleznev*. A lesser sentence, however, would cause a disparity with *Schrooten* (which
4 involved a much smaller cybercriminal enterprise and a far smaller loss amount) and with
5 *Hladyr* (which involved a defendant who was not a top-level leader and who made a
6 relatively small amount of proceeds).

7 **B. Restitution**

8 As previously noted, AT&T has calculated its losses from FAHD's misconduct at
9 \$201,497,430.94. FAHD's restitution obligation should be reduced, however, by the
10 apportioned restitution amounts agreed to by Sapatin (\$441,500), Evans, (\$280,200), and
11 Woods (\$155,032.46), and so far ordered by the Court against Evans and Woods.
12 (Sapatin's sentencing remains pending as of the date of filing of this Sentencing
13 Memorandum.) After subtracting these apportioned amounts, the Court should order
14 FAHD to pay \$200,620,698 in restitution to AT&T.⁶

15 **C. Forfeiture**

16 FAHD's Plea Agreement provides that FAHD agrees to forfeit all property that is
17 proceeds or is derived from proceeds traceable to his crime and that this includes

18 a sum of money in the amount of \$1,824,527.37, representing
19 a portion of the proceeds Defendant obtained from the
20 offense. . . . Defendant [] understands that the United States
21 will seek to forfeit a larger sum of money than \$1,824,527.37
as proceeds that Defendant obtained from the offense.

22 PA, ¶13. The government asks that the Court order a money judgment for \$5,338,430
23 (rather than the minimum \$1,824,527.37 to which FAHD has agreed).
24

25 ⁶ As previously noted, AT&T's loss calculation is set forth in a sworn Affidavit filed as Exhibit 1. AT&T has
26 permitted defense counsel to examine the witnesses who performed its analysis, and the government offered to
27 facilitate those witnesses' presence at FAHD's sentencing hearing, in the event that defense counsel wished to cross-
28 examine them, but defense counsel declined. The government believes that this is all that is required to satisfy
FAHD's due process rights and to support a restitution order. In the event the Court decides that it requires live
testimony, the government asks that the Court set a restitution hearing within the next 90 days, rather than simply
denying AT&T restitution.

1 Under controlling case law, the money judgment that the Court may enter is
2 limited to the amount of proceeds FAHD personally received from his offense. The
3 government has been limited in its ability to quantify those proceeds, because FAHD
4 conducted his banking in foreign countries from which it is difficult, if not impossible, to
5 obtain records. The government was able to identify payments from U.S. accounts
6 belonging to P.V. and/or S.V to FAHD and/or entities controlled by FAHD between June
7 3, 2013, and September 15, 2015, totaling \$1,824,527.37. A schedule of those payments
8 is attached as Exhibit 5. Fahd has agreed that those payments are payments for unlocking
9 cellular phones. *See* PA, 10. Those payments are the basis for FAHD's agreement to a
10 money judgment of at least \$1,824,527.37.

11 Although the government was not able to obtain additional relevant bank records,
12 the government did obtain evidence of additional payments to FAHD. Specifically,
13 during the investigation, the government obtained a search warrant for the account
14 fahdibrahim85@gmail.com, an email account belonging to FAHD. The Google Drive
15 storage linked to that account contained several versions of a spreadsheet titled
16 OnePlusOne.xlsx. A copy of a portion of one of those spreadsheets is attached as
17 Exhibit 6.

18 This spreadsheet appears to be an accounting of FAHD's business from February
19 2, 2015, through November 18, 2016. Among other things it contains columns with the
20 headers "Shans Payment" and "Moosani Payment." Shan is a nickname for P.V., who
21 FAHD admitted in his plea agreement purchased illegal unlocking services from FAHD.
22 *See* PA, ¶ 8. Moosani is a nickname for a person who operated a different company that
23 also used FAHD to unlock cellular phones. A sample email from Moosani to FAHD
24 providing the IMEIs of telephones to unlock, and an email response reporting on the
25 status of some of those unlocks, are attached as Exhibit 7.

26 The amounts listed as Shans Payment and Moosani Payment appear to reflect
27 payments from P.V. and/or S.V. and Moosani to FAHD for unlocking cellular
28 telephones. This can be confirmed by looking at Exhibit 8, a printout that organizes and

1 reprints data from the OnePlusOne spreadsheet. Exhibit 8 contains three columns, one
2 containing dates, and the other two headed Shans Payment and Moosani Payment. A
3 comparison of Exhibit 5 to Exhibit 8 confirms that the vast majority of payments listed in
4 the column titled Shans Payment in Exhibit 7 correspond to payments shown in Exhibit 5
5 from P.V. and/or S.V. to FAHD (although the dates listed sometimes vary slightly). It
6 also is corroborated by the fact that the investigation also has identified a number of
7 instances in which entries in the column titled Moosani Payment in Exhibit 6 correspond
8 to payments to a PayPal account opened in the name A.G. (that is, FAHD's sister) with a
9 primary email address endlesspaypal@gmail.com, and a secondary email address
10 fahdibrahim85@gmail.com (that is, FAHD's email address), which appears to be an
11 account controlled by FAHD.

12 In sum, the OnePlusOne spreadsheet is FAHD's own accounting of his unlocking
13 business, and the money that he received from that business. As shown in Exhibit 8,
14 total payments received by FAHD reflected in the OnePlusOne spreadsheet were
15 \$4,138,630. Adding this amount to the \$1,824,527.37 in Exhibit 5 (and subtracting
16 \$624,727.37 to remove payments from P.V./S.V. that are reflected in both spreadsheets),
17 FAHD's own accounting in the OnePlusOne spreadsheet, and the available bank records,
18 show that FAHD received a total of \$5,338,430 in proceeds between June 3, 2013 and
19 November 18, 2016.

20 This total certainly understates the actual amount of proceeds FAHD received
21 from his crime. For example, it does not reflect whatever proceeds FAHD received from
22 Moosani before February 2, 2015, since the OnePlusOne spreadsheet does not contain
23 information before that date. It also does not reflect proceeds FAHD received from any
24 source after November 18, 2016, since the OnePlusOne spreadsheet does not extend
25 beyond that date, even though FAHD certainly received some such proceeds (since he
26 and Woods continued unlocking cellular telephones at AT&T until at least September
27 2017). See PA, ¶ 8. Although certainly an under-reflection of FAHD's actual proceeds,
28

1 the Court should enter a money judgment in the amount of \$5,338,430 to reflect at least
2 the proceeds documented in available bank records and by FAHD's own accounting.

3
4 **V. WAIVER OF APPEAL**

5 In paragraph 16 of the plea agreement, FAHD waived his appellate rights and his
6 rights to collateral attack provided that the Court imposes a custodial sentence that is
7 within or below the Sentencing Guidelines range. Assuming the Court imposes a term of
8 incarceration that is within or below the Sentencing Guidelines range as determined by
9 the Court at the time of sentencing, the United States requests that the Court advise
10 FAHD of that fact and that he therefore has only limited remaining appellate rights,
11 following imposition of sentence.

12 //

13
14 //

15 //
16
17
18
19
20
21
22
23
24
25
26
27
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

VI. CONCLUSION

For the foregoing reasons, the Court should impose: (1) a 15-year custodial sentence with credit for time served since FAHD's arrest in Hong Kong on February 4, 2018; (2) a three-year term of supervised release; (3) a restitution judgment in the amount of \$200,620,698; (4) a forfeiture judgment in the amount of \$5,338,430; and (5) a special assessment in the amount of \$100.

DATED: this 9th day of September, 2021.

Respectfully submitted,

TESSA M. GORMAN
Acting United States Attorney

s/ Francis Franze-Nakamura
ANDREW C. FRIEDMAN
FRANCIS FRANZE-NAKAMURA
Assistant United States Attorneys
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
Telephone: (206) 553-7970
E-mail: Andrew.Friedman@usdoj.gov
Francis.Franze-Nakamura@usdoj.gov

s/ Anthony Teelucksingh
ANTHONY TEELUCKSINGH
Trial Attorney
Computer Crime & Intellectual Property Section
Department of Justice
1331 New York Avenue, N.W.
Washington, D.C. 20530
Telephone: (202) 353-4779
E-mail: Anthony.Teelucksingh@usdoj.gov

EXHIBITS

| | |
|----|---|
| 1 | Affidavit of Alfred B. Carter |
| 2 | AT&T Executive Summary (reserved) |
| 3 | Affirmation of Muhammad FAHD |
| 4 | Memorandum of Interview of FAHD |
| 5 | Schedule of Payments to FAHD |
| 6 | FAHD's "OnePlusOne" Spreadsheet |
| 7 | Email Exchange between FAHD and "Moosani" |
| 8 | Data from "OnePlusOne" Spreadsheet |
| 9 | Recorded Phone Call between Woods and FAHD (submitted separately) |
| 10 | Recorded Phone Call between Woods and FAHD (submitted separately) |